REMARKS

Claims 9-12 are pending in this application. The Examiner rejected Claims 9-12 under 35 U.S.C. § 103(a).

Geiger and Arent Do Not Teach or Suggest the Inventions of Claims 9-12

The Examiner rejected Claims 9-12 under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 6,463,534 to Geiger et al. ("Geiger") in view of U.S. Patent No. 6,018,724 to Arent ("Arent"). Applicants traverse this rejection for the reasons discussed below.

Claim 9

Geiger describes a system for secure wireless electronic commerce which enables software sales over wireless networks. The Examiner alleged that Geiger teaches a service providing system wherein the information providing server is configured to send to the authentication server information requested by the portable terminal, address information associated with the information providing server, and tag information associated with the information providing server. The Examiner also alleged that Geiger teaches a service providing system wherein the authentication server has a detector which detects whether or not the address information and tag information sent by the information providing server match the authentication information stored in the authentication information database, and cited a section of Geiger that describes cross certificates for server authentication.

The cited section of Geiger describes communication between certification authorities ("CAs"). "Cross certification is the process by which two domain root CA's issue one another cross-certificates; thereby authorizing one another's root certificates (keys)." Cross-certificates generally contain the address of one or more inter-domain validation servers and may also contain other information related to the cross-certification agreements." Column 10, lines 41-47. The cross certification described in the cited section of Geiger is performed between two CAs, not between a CA and an attribute authority ("AA"). As illustrated by Figs. 4 and 5 and as described in the cited section of Geiger, a CA communicates with

another CA in a manner similar to that used to establish roaming. To the extent that the Examiner is equating the CA of Geiger with the information provider server and the AA of Geiger to the authentication server, the cited section of Geiger does not describe the communication of information used for authentication between the CA and the AA. In particular, the cited sections of Geiger does not describe that the information providing server sends to the authentication server information requested by the portable terminal, address information associated with the information providing server, and tag information associated with the information providing server, as required by Claim 9. The cited section of Geiger also does not describe that the authentication server has a detector which detects whether or not the address information and tag information sent by the information providing server match the authentication information stored in the authentication information database, as required by Claim 9.

The Examiner admitted that Geiger fails to explicitly teach a second display area which displays the authentication information. However, the Examiner contended that the use and advantages for displaying such information is well known to one skilled in the art, as evidenced by the teachings of Arent. Arent describes displaying a certification symbol that certifies the legitimacy of the merchant, such as symbol 400 in Fig. 4. Arent describes that in response to a user's request (step 200 of Fig. 2), the requested proof of certification is provided by the merchant (step 210), and the authenticity of the provided certification is tested by using e.g. a public key system (step 230). The certification indicator 400 includes a standard symbol, such as the "digitally Certified" text shown in Fig. 5. The specific information 520 (e.g. IDX21A7) included in the certification indicator consists of "a text string, similar to password, selected by the user." Column 4, lines 58-60, emphasis added. Arent describes that an unscrupulous merchant could counterfeit the standard symbol and thus recommends the use of specific information selected by the user since that information is "not predictable and is available only on the user's local access device, [so that] it cannot be easily copied and forged by an unscrupulous merchant." Column 4, lines 47-50.

In the present invention, the authentication information displayed on the portable terminal is retrieved from the authentication database, not selected by the user. When the terminal of the present invention is used for example, as a concert ticket, the concert organizer confirms authenticity of the user's ticket by checking the content of the authentication information displayed in the second display area of the user's portable terminal. In order to do this, the authentication information displayed on the second display area needs to be determined by the information providing server or the authentication server, not the user.

The certification indicator of Arent cannot be used in the system of the present information, since the concert organizer would have no way of confirming the authenticity of the authentication information displayed in the portable terminal. Arent teaches away from the present invention because the authentication information of the present invention is for the benefit of the information provider, whereas the certification indicator of Arent is for the benefit of the user. Arent does not teach that the information displayed in the display is retrieved from the authentication database when the address information and the tag information sent from the information providing server match the stored authentication information, as required by Claim 9. Accordingly, Claim 9 would not have been obvious to one of ordinary skill from the cited references at the time Applicants made the claimed invention, and Claim 9 should be allowed.

Claim 11

Claim 11 includes similar limitations to Claim 9. For the reasons discussed above in support of patentability of Claim 9, the invention of Claim 11 also would not have been obvious to one of ordinary skill from the cited references at the time Applicants made the claimed invention. Accordingly, Claim 11 should also be allowed.

Claims 10 and 12

Claims 10 and 12 depend from independent Claims 9 and 11 respectively. The remarks made above in support of patentability of the independent claims are equally applicable to distinguish the dependent claims from the cited references.

Geiger and Kolev Do Not Teach or Suggest the Inventions of Claims 9-12

The Examiner also rejected Claims 9-12 under 35 U.S.C. § 103(a) as unpatentable over Geiger in view of Kolev et al. ("Kolev"). Applicants traverse this rejection for the reasons discussed below.

Claim 9

As discussed above in relation to the patentability of Claim 9 over Geiger and Arent, the cited section of Geiger does not describe that the information providing server sends to the authentication server information requested by the portable terminal, address information associated with the information providing server, and tag information associated with the information providing server, as required by Claim 9. The cited section of Geiger also does not describe that the authentication server has a detector which detects whether or not the address information and tag information sent by the information providing server match the authentication information stored in the authentication information database, as required by Claim 9.

The Examiner admitted that Geiger fails to explicitly teach a second display area which displays the authentication information. However, the Examiner contended that the use and advantages for displaying such information is well known to one skilled in the art, as evidenced by the teachings of Kolev.

The invention of Kolev is related to authentication, which it defines as subscription verification, and confirmation and ciphering, which it defines as subscriber identity and data/voice communication confidentiality. Column 4, lines 48-52. Kolev describes a communication device 10 for a digital wireless network 11 having a display 22, which

displays an authentication indicator 24 only when the communication device is authenticated. Column 5, lines 17-35. Kolev describes that the authentication indicator 24 may be a text message, an icon, a light, or an alpha numeric message. Column 5, lines 36-39. There is no teaching in Kolev that the information displayed in the display is retrieved from an authentication database when the address information and the tag information sent from the information providing server match the stored authentication information, as required by Claim 9. As such, the combination of Geiger and Kolev does not teach the service providing system of Claim 9, and Claim 9 would not have been obvious to one of ordinary skill from the cited references at the time Applicants made the claimed invention. Thus, Claim 9 is also patentable over Geiger and Kolev.

Claim 11

Claim 11 includes similar limitations to Claim 9. For the reasons discussed above in support of patentability of Claim 9, the invention of Claim 11 also would not have been obvious to one of ordinary skill from the cited references at the time Applicants made the claimed invention. Accordingly, Claim 11 should also be allowed.

Claims 10 and 12

Claims 10 and 12 depend from independent Claims 9 and 11 respectively. The remarks made above in support of patentability of the independent claims are equally applicable to distinguish the dependent claims from the cited references.

Kiessling and Hamalainen Do Not Show or Suggest the Invention of Claims 9-12

The Examiner requested Applicants to consider U.S. Patent No. 6,901,251 to Kiessling et al. ("Kiessling") and U.S. Patent No. 6,249,584 to Hamalainen et al. ("Hamalnen") for relevant teachings when responding to the Office Action. Applicants have

considered the teachings of these references and submit that none of the references describe the invention of Claim 9.

In particular, Kiessling describes displaying authentication information, such as "Security OK" at 22b of Fig. 4a. The invention of Kissling is similar to that described by Arent in that it describes secure online transactions using a wireless terminal. Kiessling merely displays fixed authentication information, such as "Security OK", and does not teach that the information displayed in the display is retrieved from the authentication database when the address information and the tag information sent from the information providing server match the stored authentication information, as required by Claim 9.

Hamalainen describes monitoring signals transferred between a mobile communication network and a mobile station, and indicating the cipher mode to the user of the mobile station. The cipher mode is indicated by emitting or flashing a light source, such as a light-emitting diode (LED) or by vibrating vibration batteries. Column 7, lines 66 to Column 8, line 24. The cipher mode is displayed only to indicate whether or not enciphering of data transmission exists. Hamalainen also fails to describe that the information displayed in the display is retrieved from the authentication database when the address information and the tag information sent from the information providing server match the stored authentication information, as required by Claim 9.

Claim 11 includes similar limitations to Claim 9 and Claims 10 and 12 depend from independent Claims 9 and 11 respectively. For the reasons discussed above, these claims also would not have been obvious to one of ordinary skill from the cited references at the time Applicants made the claimed invention. Accordingly, Claims 9-12 should be allowed.

CONCLUSION

The foregoing is submitted as a complete response to the Office Action identified above. This application should now be in condition for allowance, and the Applicant solicits a notice to that effect. If there are any issues that can be addressed via telephone, the Examiner is asked to contact the undersigned at 404.685.6799.

Respectfully submitted,

Brenda O. Holmes

By: Brenda O. Holmes
Reg. No. 40,339

KILPATRICK STOCKTON LLP
1100 Peachtree Street, Suite 2800
Atlanta, Georgia 30309-4530
Telephone: (404) 815-6500
Facsimile: (404) 815-6555
Our Docket: 44471-234039 (13700-0235)